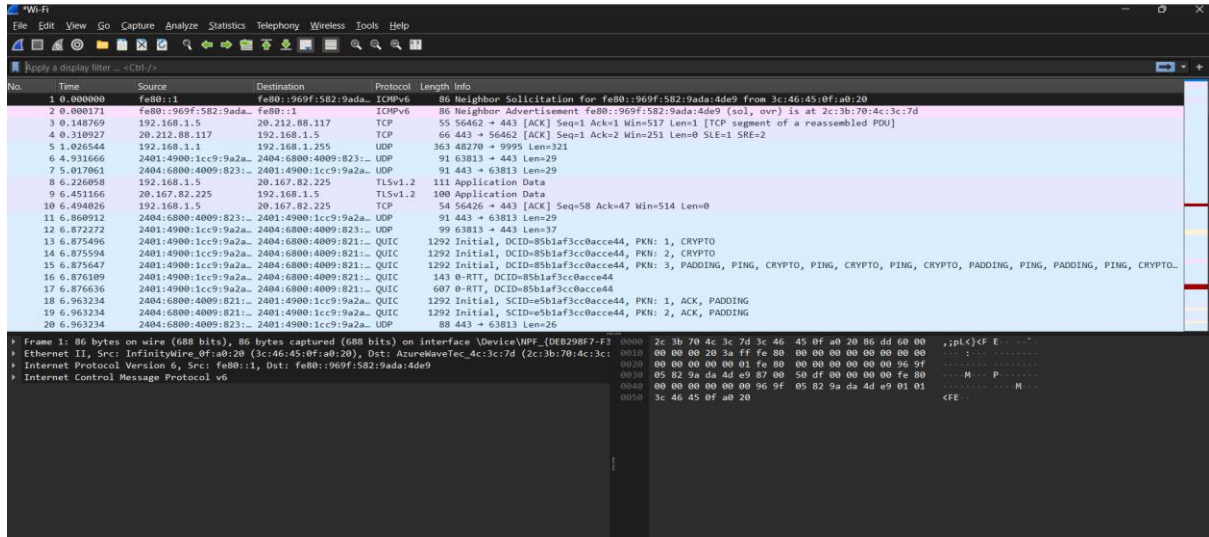


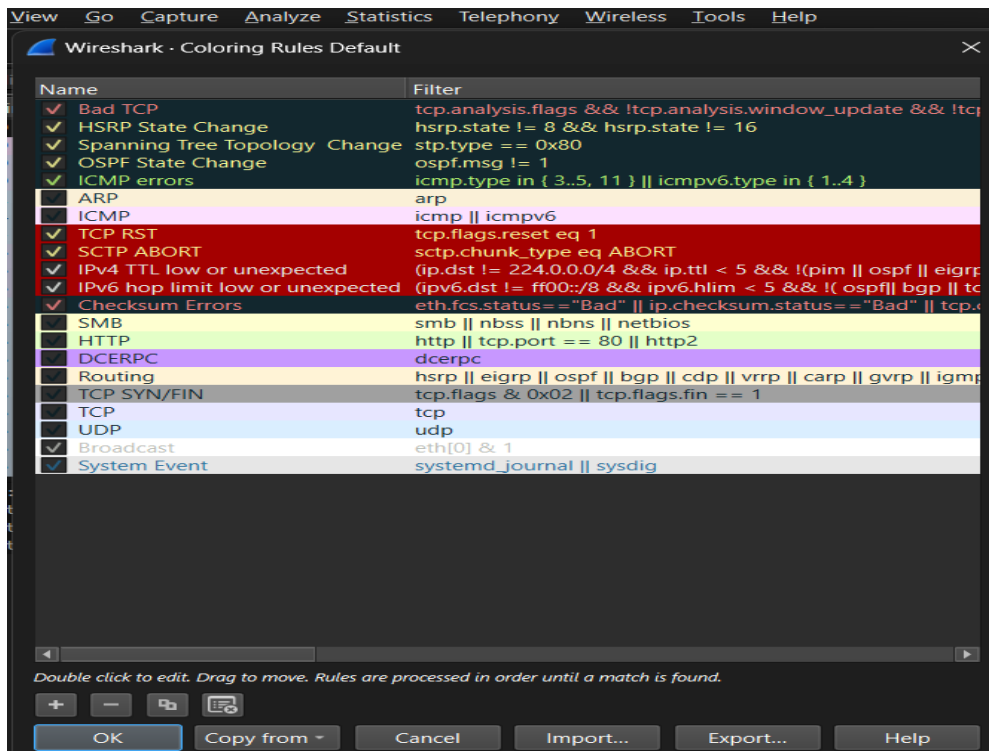
## Practical -5

### Experiments on Packet capture tool: Wireshark

#### Capturing Packets



#### Color Coding



## Filtering Packets

*Wi-Fi									
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									
tcp									
No.	Time	Source	Destination	Protocol	Length	Info			
3	0.148769	192.168.1.5	20.212.88.117	TCP	55	56462 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reassembled PDU]			
4	0.310927	20.212.88.117	192.168.1.5	TCP	66	443 → 56462 [ACK] Seq=1 Ack=2 Win=251 Len=0 SLE=1 SRE=2			
8	6.226058	192.168.1.5	20.167.82.225	TLSv1.2	111	Application Data			
9	6.451166	20.167.82.225	192.168.1.5	TLSv1.2	100	Application Data			
10	6.494026	192.168.1.5	20.167.82.225	TCP	54	56426 → 443 [ACK] Seq=58 Ack=47 Win=514 Len=0			
49	8.313251	13.107.42.12	192.168.1.5	TCP	54	443 → 56523 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
80	13.312192	13.107.42.12	192.168.1.5	TCP	54	443 → 56524 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
81	13.312192	13.107.42.12	192.168.1.5	TCP	54	443 → 56525 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0			
86	14.828760	2401:4900:1cc9:9a2a::	2603:1040:a06:6::2	TCP	75	49590 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1 [TCP segment of a reassembled PDU]			
88	15.056202	2603:1040:a06:6::2	2401:4900:1cc9:9a2a::	TCP	86	443 → 49590 [ACK] Seq=1 Ack=2 Win=6949 Len=0 SLE=1 SRE=2			
91	16.234855	2401:4900:1cc9:9a2a::	2404:6800:4003:c01::	TCP	75	56463 → 5228 [ACK] Seq=1 Ack=1 Win=512 Len=1			
93	16.290367	2404:6800:4003:c01::	2401:4900:1cc9:9a2a::	TCP	86	5228 → 56463 [ACK] Seq=1 Ack=2 Win=290 Len=0 SLE=1 SRE=2			

## TCP Stream

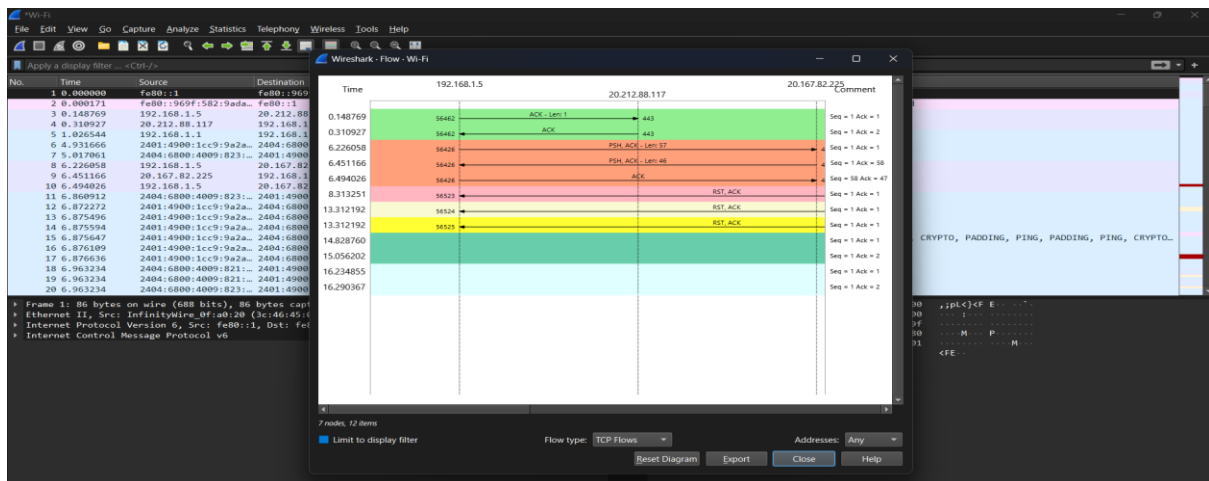
*Wi-Fi									
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									
tcp.stream eq 1									
No.	Time	Source	Destination						
8	6.226058	192.168.1.5	20.167.82.225						
9	6.451166	20.167.82.225	192.168.1.5						
10	6.494026	192.168.1.5	20.167.82.225						

Frame 9: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0  
Ethernet II, Src: InfinityWire\_0f:a0:20 (3c:46:45:0f:a0:20), Dst: 20:167:82:225  
Internet Protocol Version 4, Src: 20.167.82.225, Dst: 192.168.1.5  
Transmission Control Protocol, Src Port: 443, Dst Port: 56426

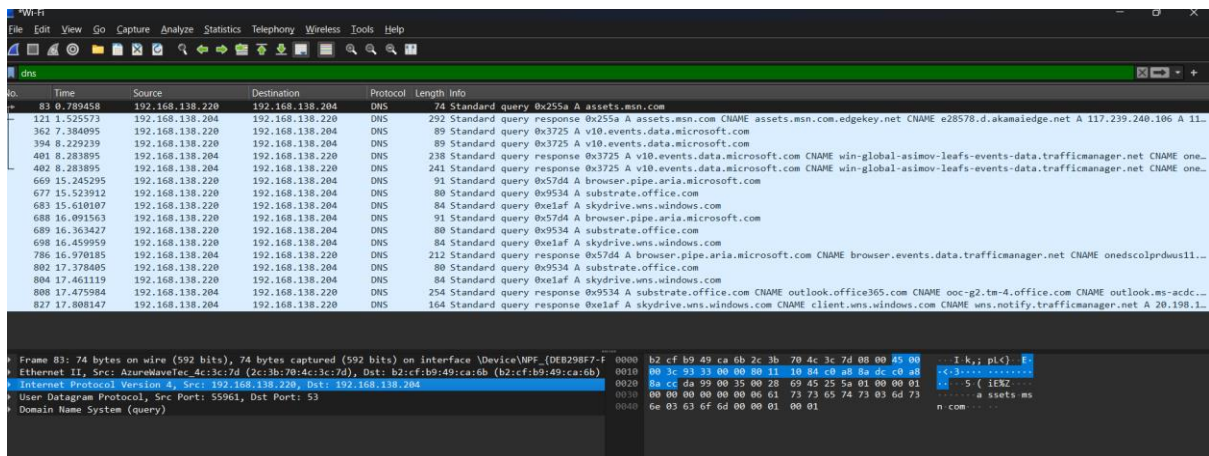
...4.....4  
1.  
...q.?2...?...Q1.....ar...!..h....Y.+G\_...U...:.....).....N.....'z...7+4oB...>...f  
..5?.....

00 20 08 00 45 00 ;pL<}<F E...E  
14 a7 52 e1 c0 a8 V9t@ p...R..  
16 be c3 9c 50 18 ....j-P --6..P  
19 00 00 00 00 00 .....-)).....

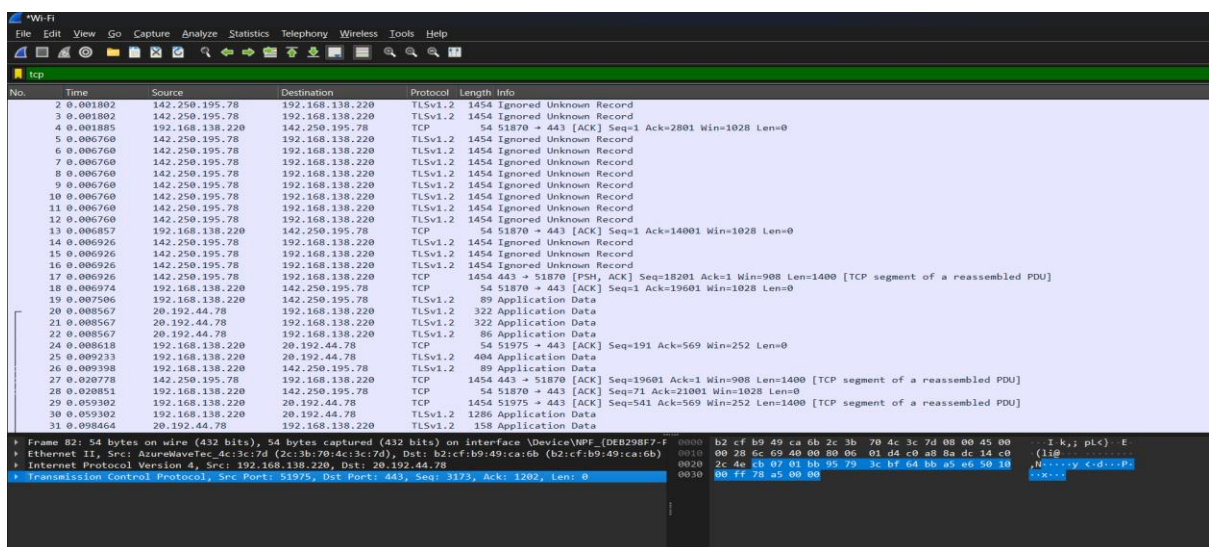
## Flow Graph:



## DNS:



## TCP



ARP

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
283	5.417405	b2:cf:b9:49:ca:6b	AzureWaveTec_4c:3c:7d	ARP	42	Who has 192.168.138.220? Tell 192.168.138.204
284	5.417445	AzureWaveTec_4c:3c:7d	b2:cf:b9:49:ca:6b	ARP	42	192.168.138.220 is at 2c:3b:70:4c:3c:7d

Frame 283: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF\_{DEB298F7-0000-0000-0000-000000000000} 2c 3b 70 4c 3c 7d b2 cf b9 49 ca 6b 08 06 00 01 ;;pL<... I k....

Ethernet II, Src: b2:cf:b9:49:ca:6b (b2:cf:b9:49:ca:6b), Dst: AzureWaveTec\_4c:3c:7d (2c:3b:70:4c:3c:7d) 0010 08 00 06 04 00 01 b2 cf b9 49 ca 6b c0 a8 8a cc ..... I k....

Address Resolution Protocol (request) 0020 00 00 00 00 00 c0 a8 8a dc ..... ..